UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE INGENIERÍA

CARRERA DE ESPECIALIZACIÓN EN SISTEMAS EMBEBIDOS

MEMORIA DEL TRABAJO FINAL

Módulo de conectividad WiFi/Bluetooth para electrodomésticos

Autor:
Ing. Matías Nicolás Brignone

Director:
Esp. Ing. Diego Fernández (FIUBA)

Jurados:
Mg. Ing. Gonzalo Sánchez (FIUBA, FAA)
Esp. Ing. Matías Álvarez (FIUBA)
Esp. Ing. Santiago Germino (FIUBA)

Este trabajo fue realizado en la ciudad de Córdoba, entre marzo de 2019 y abril de 2020.

Resumen

En la presente memoria se describe el desarrollo de un módulo que permite dotar de conectividad WiFi y Bluetooth a un electrodoméstico, a los fines de permitir su manejo remoto por parte del usuario final. También permite la recopilación de información de uso y estado por parte del fabricante del electrodoméstico. Con el objetivo de agilizar el desarrollo, el electrodoméstico a controlar se emula con un microcontrolador con el que se comunica el módulo.

Para desarrollar el trabajo se utilizaron un sistema operativo de tiempo real, diferentes protocolos de comunicación en distintas capas (WiFi/Bluetooth para la capa física, HTTPS/MQTT para la capa de aplicación, entre otros), sistemas de control de versiones y herramientas de gestión de proyectos.

Agradecimientos

A mi familia, por su constante apoyo.

A mis amigos y colegas, por acompañarme en este camino.

Índice general

Índice de figuras

Índice de Tablas

Dedicado a mi familia.

Capítulo 1

Introducción General

En este capítulo se realiza una introducción al concepto de Internet de las Cosas, se describe la motivación del trabajo realizado y se presentan sus objetivos y alcance.

1.1. Internet de las Cosas

Desde la aparición de Internet a finales del siglo pasado, ha quedado demostrado lo útil que es contar con un dispositivo capaz de conectarse a la red. Los beneficios de que una computadora o un teléfono inteligente puedan conectarse a Internet son evidentes, y esos beneficios también se encuentran presentes al conectar cualquier otro objeto a Internet, y es allí donde surge el concepto de Internet de las Cosas (IoT, por sus siglas en inglés correspondientes a *Internet of Things*).

La Internet de las Cosas consiste en extender el potencial de Internet y la conectividad más allá de las computadoras y celulares, e incorporar a todos los objetos (cosas) de la vida cotidiana y que se encuentran presentes en el entorno de una persona. Así se permite tanto la comunicación e interacción entre sí de estos objetos, como así también el monitoreo y control en forma remota.

El concepto de «cosa» es sumamente amplio, ya que contempla desde lámparas, cerraduras y termostatos en el hogar, hasta maquinaria industrial y sistemas de riego para agricultura, pasando por vehículos autónomos, sistemas de iluminación y sensores para estacionamiento público en una ciudad. El objeto conectado incluso puede ser un monitor cardíaco en el interior de una persona o un chip insertado en un animal de granja. Gracias a la existencia de sensores y microcontroladores cada vez más potentes, más pequeños y de menor costo, es posible lograr que prácticamente cualquier dispositivo forme parte del ecosistema IoT.

Los beneficios que la Internet de las Cosas ofrece tanto a empresas como a personas individuales son innumerables. Desde un punto de vista económico, les da la posibilidad a las empresas de conocer y monitorear mejor sus procesos, para así hacerlos más eficientes y posibilitar mejores tomas de decisiones y acciones como mantenimiento predictivo de maquinaria. Todo eso se traduce en definitiva en un ahorro de dinero y tiempo para la organización. Con respecto a un individuo particular, la Internet de las Cosas le permite mejorar su calidad de vida y su comodidad en el día a día con automatizaciones en el hogar (domótica), como así también beneficios a la salud con, por ejemplo, implantes inteligentes que permiten un cuidadoso monitoreo.

Las empresas, las personas y el mercado en general hace ya varios años que se han dado cuenta de la importancia de la Internet de las Cosas. Es prueba de ello la gran cantidad de dispositivos conectados que existen, y las proyecciones que indican que estos números seguirán aumentando notablemente. En 2017 ya había 27 mil millones de dispositivos IoT conectados, cifra que aumentará a un ritmo de un 12 % anual hasta llegar a 125 mil millones para 2030 [1]. Por otra parte, en la figura 1.1 se puede observar cómo el mercado mundial de la Internet de las Cosas ya maneja cantidades de dinero superiores a los USD 200.000.000.000, y cómo esa cifra aumentará sustancialmente a lo largo de los próximos años [2], lo cual supone una enorme oportunidad de negocio para muchas empresas.

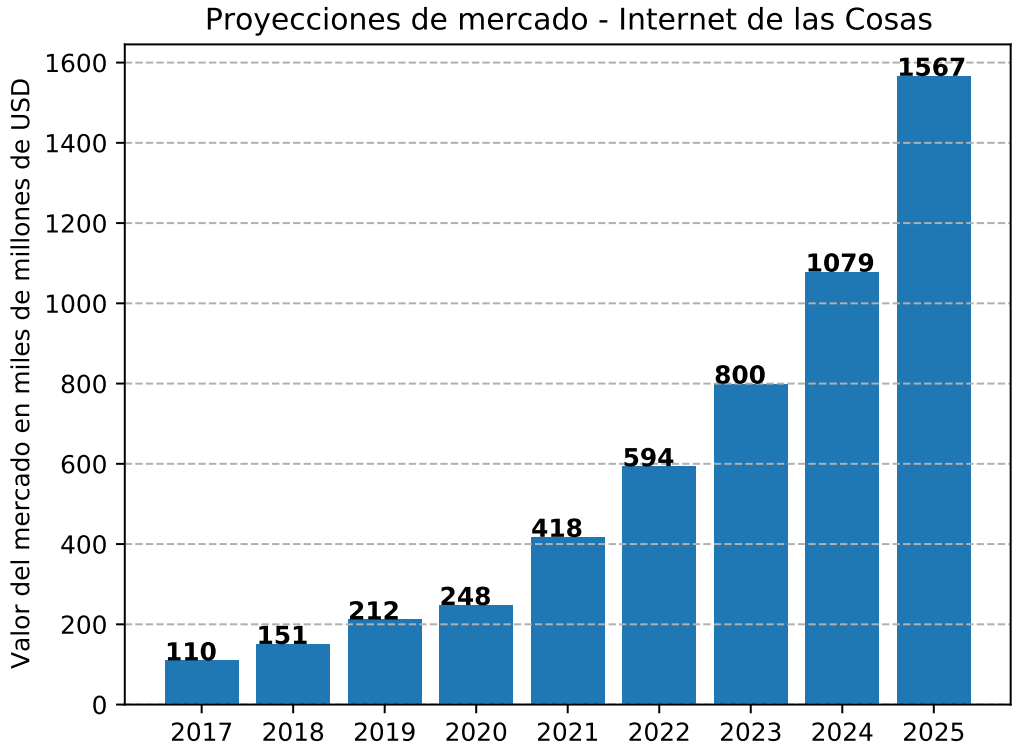

FIGURA 1.1: Proyecciones del valor de mercado a nivel mundial de la Internet de las Cosas.[1]

Por último, un punto que a menudo es pasado por alto al momento de hablar de la Internet de las Cosas, son todos los problemas asociados a la seguridad y la privacidad. Tener un mayor número de dispositivos conectados, muchos de los cuales recolectan información sumamente sensible, expande la superficie de ataque considerablemente, y deja tanto a empresas como a personas más vulnerables frente a posibles ciberdelincuentes. Existen incontables ejemplos de vulnerabilidades en dispositivos IoT que salieron a la luz, como una gigantesca *botnet* formada por dispositivos IoT [3], televisores inteligentes que espían conversaciones privadas [4], e incluso ataques dirigidos a dispositivos conectados en entornos industriales [5]. Estos hechos ocurren principalmente porque la seguridad y la privacidad a menudo son vistas como costos extra en los que no vale la pena incurrir. Incluso en ocasiones la propia empresa utiliza de manera poco ética esos

[1]Gráfico replicado en base al que se muestra en https://www.statista.com/statistics/976313/global-iot-market-size/.

agujeros de seguridad para obtener datos de los usuarios y sacar algún tipo de provecho económico a partir de ellos.

Las consecuencias de una falla de seguridad en un dispositivo IoT pueden ser muy graves, por lo que al momento de desarrollar una solución en el segmento del Internet de las Cosas, los aspectos de seguridad deben ser tenidos en consideración desde un principio, aún cuando ello implique desarrollar un producto más costoso o complejo.

1.2. Estado del arte

En la actualidad, existe una enorme cantidad de dispositivos conectados que pertenecen a muy diversos ámbitos, por lo que resultaría poco práctico brindar un panorama general del estado del arte en todos ellos. Por lo tanto, el foco estará en aquellos productos que ofrezcan soluciones orientadas a dispositivos que ya cuentan con cierto nivel de "inteligencia" (como maquinaria industrial/agrícola o artefactos del hogar), a los fines de dotarlos de conectividad y de todo un entorno que permita procesar y analizar los datos generados por ellos.

Por un lado, existen numerosas plataformas que solamente ofrecen la etapa de procesamiento, análisis y visualización de datos. Estas plataformas asumen que el cliente cuenta con el hardware necesario para enviarles la información relevante, y ellas se encargan de analizarla y presentarla de manera conveniente mediante tableros o *dashboards*, que le permiten al usuario ver el estado de los dispositivos y actuar sobre ellos. La mayoría de estas plataformas poseen características similares tales como administración de dispositivos, visualización de datos y soporte a múltiples protocolos de comunicación. Algunos ejemplos de esta clase de plataformas son ThingBoard [6], Thinger [7] y Ubidots [8], además de los servicios específicamente orientados a IoT de Amazon Web Services, de Google Cloud Platform y de Microsoft Azure.

Por otra parte, existen también plataformas de hardware que ofrecen soluciones genéricas de conectividad, junto con plataformas para analizar y visualizar los datos obtenidos, con características similares a las mencionadas anteriormente.

En este último segmento hay diferentes grados de especialización. Por ejemplo, existen empresas que ofrecen soluciones orientadas exclusivamente al ámbito industrial, como ThingWorx de la empresa PTC [9], mientras que otras brindan soluciones más genéricas con una plataforma de hardware y un entorno de análisis y visualización, como el caso de Particle (figura 1.2) [10].

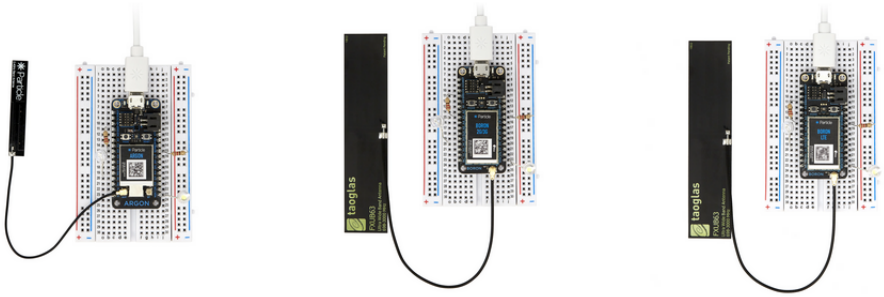

FIGURA 1.2: Plataformas de hardware ofrecidas por Particle.[2]

1.3. Motivación

Un sector fundamental en el ámbito del Internet de las Cosas es el de la domótica, es decir el conjunto de tecnologías que permite el control y la automatización inteligente de una vivienda, a los fines de lograr una gestión eficiente y brindar mayor comodidad y seguridad a quienes la habitan [11].

A su vez, dentro de la domótica, un campo de especial interés es el de los electrodomésticos inteligentes (o *smart appliances*), tales como televisores, heladeras, hornos, lavarropas o microondas.

Una característica primordial de un electrodoméstico inteligente es su capacidad de estar conectado y ser manejado o accedido de forma remota, ya sea mediante una plataforma web, una aplicación en el celular, comandos de voz o cualquier otro medio. Esta capacidad brinda grandes ventajas con respecto a un artefacto convencional, ya que no solamente ofrece una mayor comodidad al momento de usarlo, sino que también permite programar acciones (como preparar un café a una determinada hora) y ahorrar energía al hacer más eficiente su uso.

Actualmente existen ya en el mercado numerosos ejemplos de electrodomésticos inteligentes que permiten llevar a cabo diferentes acciones:

- Encender el horno mediante un comando de voz, incluso con integración con los asistentes de voz más comunes.
- Consultar el contenido de la heladera mediante una aplicación en el celular.
- Recibir una notificación cuando el ciclo de lavado del lavarropas finaliza.
- Diagnosticar automáticamente la causa de una falla.

Gracias a las ventajas que ofrecen, la demanda de electrodomésticos inteligentes es cada vez más mayor, por lo que aquellas empresas o fabricantes que no se modernicen y comiencen a incorporar características *smart* a sus dispositivos, se encontrarán en clara desventaja al competir en el mercado con aquellas que sí lo hagan.

Como se puede apreciar en la sección 1.2, existen ya en el mercado numerosas soluciones orientadas a la Internet de las Cosas. Cada una de ellas ofrece diferentes características y cubre diferentes mercados. Dentro de las soluciones que ofrecen una plataforma tanto de hardware como de software, no existe un sector consolidado que esté orientado a dotar de conectividad a electrodomésticos en el hogar, y es allí donde surge la importancia del presente trabajo. Lo que se busca es cubrir justamente ese sector y ofrecer una solución personalizada a los fabricantes para que puedan lograr que los electrodomésticos que ya fabrican se conviertan en electrodomésticos inteligentes.

[2]Imagen extraída de https://store.particle.io/pages/prototyping-hardware.

1.4. Objetivos y alcance

1.4.1. Objetivos generales

El objetivo general del presente trabajo es el diseño e implementación de un módulo capaz de dotar de conectividad WiFi y Bluetooth a un electrodoméstico convencional. Para ello, el módulo debe tener la capacidad de comunicarse con la placa del propio equipo y de recibir/enviar información a un servidor en la nube, a los fines de permitirle al usuario final un manejo remoto del aparato y conocer su estado, como así también enviar información de uso al fabricante.

El módulo no está destinado directamente al usuario final del electrodoméstico, sino a empresas o fabricantes que busquen incorporar características inteligentes a sus electrodomésticos.

A grandes rasgos, desde el punto de vista del usuario final, se debe permitir:

- Enviar por WiFi o Bluetooth un comando al electrodoméstico que dispare una acción en él, como iniciar la cocción en un horno o el lavado en un lavarropas.
- Conocer el estado del electrodoméstico mediante la recepción de información por WiFi o Bluetooth.

Por otra parte, desde el punto de vista del fabricante del electrodoméstico se debe permitir:

- Recibir y almacenar información acerca del estado de todos los dispositivos (si están o o no conectados, y en qué estado de ejecución se encuentran).
- Analizar y visualizar de manera conveniente la información de estado de los dispositivos a lo largo del tiempo.

1.4.2. Alcance

El presente trabajo incluye los siguientes aspectos:

1. Análisis, investigación y elección del hardware a utilizar en el módulo.
2. Implementación del firmware del sistema.
3. Comunicación con un microcontrolador que emule el comportamiento del electrodoméstico.
4. Desarrollo de una interfaz web mediante una plataforma ya existente, que permita enviarle comandos al electrodoméstico emulado.
5. Implementación de un entorno en la nube que permita analizar y visualizar los datos de los diferentes electrodomésticos conectados.

Es de especial importancia el punto 3 de la lista, en el que se define explícitamente que, a los fines de agilizar considerablemente el tiempo de desarrollo del trabajo, el prototipo no se utilizará en un electrodoméstico real. La interacción con él se emula mediante la comunicación con otro microcontrolador, que actúa como la placa de control del electrodoméstico: imita su comportamiento y sus respuestas ante diferentes estímulos.

En línea con el párrafo anterior, el presente trabajo no incluye lo siguiente:

1. Integración del prototipo a diferentes electrodomésticos/marcas con distintos tipos de comunicación serie y funcionalidades.
2. Desarrollo de una aplicación móvil desde la cual interactuar por Bluetooth con el módulo.
3. Diseño y fabricación de un circuito impreso. Para el trabajo se utiliza una placa de prototipo ya existente que incluye el hardware seleccionado.

Capítulo 2

Introducción Específica

En el presente capítulo se brinda una explicación del funcionamiento general del sistema implementado, como así también una introducción a diferentes tecnologías utilizadas en el trabajo. Se presentan además los requerimientos y la planificación del trabajo.

2.1. Funcionamiento general del sistema

Como se mencionó en el capítulo 1, el propósito del presente trabajo es el desarrollo de un módulo capaz de dotar de conectividad WiFi/Bluetooth a un electrodoméstico convencional. Para que ello sea posible, es necesario contar con diferentes módulos, tal como puede observarse en la figura 2.1, en la que se presenta un diagrama de bloques del sistema implementado.

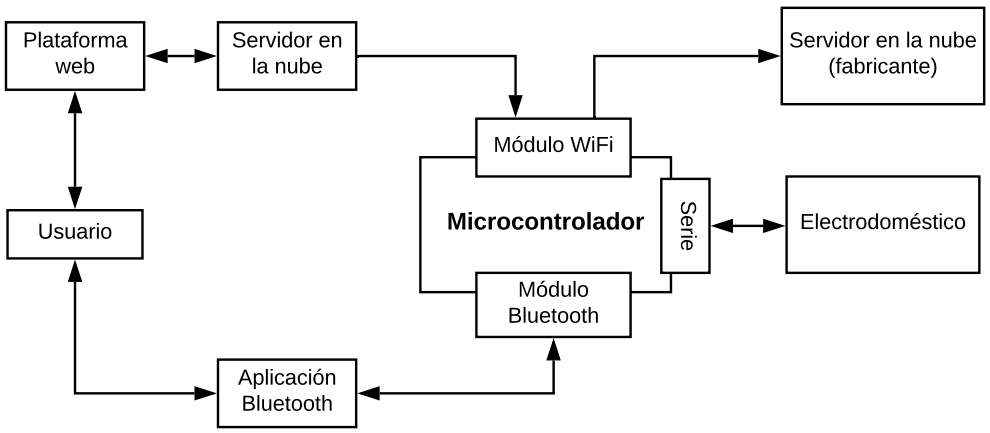

FIGURA 2.1: Diagrama general del sistema implementado.

El principal componente del sistema es el microcontrolador, que se encarga de procesar los comandos recibidos y de gestionar todas las comunicaciones, para lo cual hace uso de sus interfaces de comunicación (módulos WiFi, Bluetooth y serie).

Para ilustrar el funcionamiento general del sistema, se presenta a continuación la serie de acciones que tiene lugar en un caso de uso típico del sistema, en el que el usuario desea que el electrodoméstico inicie una determinada operación (como por ejemplo, el ciclo de lavado en un lavarropas).

- El usuario final le envía un comando al electrodoméstico, desde su computadora o celular.
  - En caso de que el comando sea enviado por WiFi, la comunicación pasa a través de un servidor en la nube que recibe el comando del usuario y luego lo envía al microcontrolador.
  - En caso de que el comando sea enviado por Bluetooth, la comunicación se realiza de manera directa con el microcontrolador.
- El módulo correspondiente (módulo WiFi o Bluetooth, según sea el caso) recibe el comando y le informa al microcontrolador que hay un nuevo comando pendiente para procesar.
- El microcontrolador procesa el comando recibido y determina la acción a ejecutar.
- Si la acción a ejecutar lo requiere, el microcontrolador se comunica con la placa de control del electrodoméstico mediante una interfaz serie, a los fines de disparar en el mismo la operación deseada por el usuario.
- Dependiendo del tipo de acción, el electrodoméstico puede contestar con su información de estado, la cual es recibida por el microcontrolador y enviada de vuelta al usuario, a través de la misma interfaz desde la cual recibió el comando originalmente. Es decir, que si el usuario envió un comando por Bluetooth para consultar el estado del artefacto, el microcontrolador utiliza el módulo Bluetooth para devolverle la respuesta.

Cabe mencionar que, debido a limitaciones de hardware, las interfaces de comunicación WiFi y Bluetooth no pueden ser utilizadas en simultáneo. Por lo tanto, si se envían comandos por WiFi, el Bluetooth debe estar apagado, y viceversa al enviar comandos por Bluetooth.

De manera independiente a las acciones disparadas a partir de un comando del usuario, el microcontrolador envía periódicamente al fabricante información acerca del estado del electrodoméstico. Este envío se lleva a cabo mediante la interfaz WiFi, que se comunica con un servidor en la nube solamente accesible por el fabricante, y que se encarga de almacenar la información para luego permitir su análisis y visualización. Gracias a esta información, el fabricante puede conocer y visualizar en todo momento el estado de sus electrodomésticos, ya sea de manera individual con todo el historial de uso de cada uno, o de forma general agrupando artefactos para obtener un panorama global del estado de sus dispositivos conectados.

Además, el módulo crea y mantiene activa en todo momento una red WiFi local de corto alcance en la que se encuentra corriendo un servidor web. El usuario puede conectarse a esta red y luego acceder desde cualquier navegador de Internet al servidor web, el cual permite configurar las credenciales de la red WiFi doméstica a la cual el módulo se conectará para recibir comandos y enviar información de uso al fabricante.

2.2. Tecnologías inalámbricas

En la actualidad, existen numerosas tecnologías inalámbricas que son aplicables a la Internet de las Cosas, muchas de las cuales incluso surgieron debido a la relevancia que este concepto fue tomando, como es el caso de NB-IoT [12], LoRa [13] y SigFox [14]. Muchas de estas tecnologías se caracterizan por permitir un bajo consumo de potencia y un largo alcance, a costa de una baja velocidad de transmisión, lo cual en muchas ocasiones es una relación de compromiso ideal para Internet de las Cosas.

A pesar del surgimiento de estas nuevas redes, las tecnologías tradicionales de conectividad inalámbrica, como el WiFi [15] y el Bluetooth [16], siguen siendo adecuadas para muchas aplicaciones, especialmente aquellas que requieren una interacción directa con el usuario final. Esto se debe a que son tecnologías ampliamente soportadas por la gran mayoría de los dispositivos que posee una persona, como computadoras y celulares.

Un electrodoméstico conectado interactúa de manera directa con la persona que lo utiliza en el hogar, por lo tanto el WiFi y el Bluetooth son tecnologías sumamente adecuadas para un módulo destinado a tal fin.

La tecnología WiFi permite transmitir a grandes velocidades, pero con un alcance bajo y un consumo de energía mayor. Esto último impide que el WiFi sea utilizado en, por ejemplo, sensores que funcionan a batería ubicados en lugares remotos, pero no supone un problema para un electrodoméstico que se encuentra en el hogar, con fácil acceso a una fuente de alimentación y cerca de un punto de acceso al cual conectarse.

Las especificaciones del WiFi definen una interfaz que se emplea para enviar y recibir señales entre un dispositivo inalámbrico (estación WiFi) y un punto de acceso. Si además se requiere tener acceso a Internet, es necesario conectarse también con un *router* y un módem, el cual a su vez debe estar conectado a un proveedor de servicios de Internet (ISP, por sus siglas en inglés correspondientes a *Internet Service Provider*). El módulo en el electrodoméstico actúa como una estación WiFi, es decir como un dispositivo que se conecta a la red doméstica de la casa y a través de ella obtiene una salida a Internet.

Por su parte, la tecnología Bluetooth pertenece a otro tipo de redes, denominadas Redes de Área Personal (PAN, por sus siglas en inglés) [ref]. Una conexión Bluetooth permite la comunicación directa entre dos dispositivos cercanos y su uso está sumamente masificado, ya que es fácil y económico integrarlo en muchos aparatos. Estas son características que lo convierten en una tecnología ideal para utilizar en un electrodoméstico conectado.

Su utilización en el ámbito de la Internet de las Cosas cobró verdadera importancia gracias al surgimiento del Bluetooth Low Energy (BLE) [ref], el cual fue diseñado específicamente para proporcionar un bajo consumo de energía. Esto permitió incrementar aún más la popularidad de la tecnología, extendiéndola hacia nuevos dispositivos como relojes o incluso zapatillas, lo cual fue acompañado con cada vez más modelos de computadores y celulares que también soporten la tecnología.

2.3. Protocolos HTTP/S y MQTT

Para que un dispositivo pueda conectarse a Internet, necesariamente debe recurrir al modelo TCP/IP [17], cuyas diferentes capas pueden observarse en la figura 2.2.

FIGURA 2.2: Capas del modelo TCP/IP.

El protocolo a nivel de capa de acceso a la red depende del hardware y del tipo de conectividad del dispositivo, y en el caso de este trabajo está constituida por la tecnología WiFi. Las capas de Internet y de transporte utilizan, en este trabajo, los protocolos que le dan el nombre al modelo, es decir IP (*Internet Protocol*) y TCP (*Transmission Control Protocol)*) respectivamente.

La capa de aplicación, ubicada en la parte superior del modelo, es la encargada de ofrecerle a las aplicaciones de usuario la posibilidad de comunicarse con otros dispositivos a través de los servicios brindados por las demás capas.

El protocolo de aplicación más conocido es el Protocolo de Transferencia de Hipertexto (HTTP por sus siglas en inglés, correspondientes a *Hypertext Transfer Protocol*), el cual tiene una estructura cliente-servidor y permite realizar peticiones de datos y recursos [18]. Este protocolo es la base de cualquier intercambio de datos en la web, y por lo tanto es utilizado en aplicaciones de Internet de las Cosas cuando se desea que el dispositivo conectado acceda directamente a diferentes páginas web.

Existe una variante denominada Protocolo Seguro de Transferencia de Hipertexto (HTTPS por sus siglas en inglés, correspondientes a *Hypertext Transfer Protocol Secure*), que como su nombre lo indica, es una versión segura de HTTP en la que la transmisión está encriptada y el servidor autenticado [19]. En toda aplicación, siempre se debe hacer lo posible para utilizar HTTPS y no simplemente HTTP, para garantizar la seguridad y la privacidad de los datos.

Además de los protocolos HTTP y HTTPS, existen otros protocolos para la capa de aplicación con características que los hacen ideales para la Internet de las Cosas, entre los que se destaca el protocolo MQTT (*Message Queue Telemetry Transport*) [20]. Este protocolo se basa en un modelo de publicaciones y subscripciones, en el que un cliente publica mensajes en un tema o *topic*, y todos aquellos nodos que se encuentran subscriptos a ese tema, reciben el mensaje publicado. MQTT es ideal para aplicaciones de IoT, debido principalmente a que requiere un muy bajo ancho de banda, tiene un menor consumo de potencia que otras alternativas, y además es sencillo y ligero de implementar.

Por todo lo enunciado anteriormente es que se decide que el módulo desarrollado soporte los 3 protocolos: HTTP, HTTPS y MQTT.

2.4. Requerimientos

A continuación se presentan los requerimientos en base a los cuales se desarrolló el presente trabajo, agrupados en cuatro categorías.

1. Requerimientos generales del sistema.
   - *a*) El módulo debe ser capaz de llevar a cabo, mediante la recepción de comandos por WiFi o Bluetooth, las mismas funciones que a través de la interfaz física del electrodoméstico.
   - *b*) El módulo debe ser capaz de enviar comandos por WiFi o Bluetooth, transmitiendo información de estado del electrodoméstico.
   - *c*) Las acciones a ejecutar de acuerdo al comando recibido dependen de cada aparato en particular, pero como mínimo se debe brindar la posibilidad de iniciar o detener la acción del electrodoméstico y consultar su estado.
   - *d*) El módulo debe enviar al fabricante información asociada al uso del electrodoméstico, incluyendo el envío periódico del estado en el que se encuentra.
   - *e*) El módulo debe ser capaz de crear su propia red local WiFi a los fines de permitir configurar las credenciales de de la red WiFi a conectarse.
   - *f*) El módulo debe ser capaz de enviar y recibir comandos por WiFi utilizando los protocolos HTTP, HTTPS y MQTT.
2. Requerimientos de hardware.
   - *a*) El módulo debe poder comunicarse utilizando el Estándar IEEE 802.11 b/g/n (WiFi).
   - *b*) El módulo debe poder comunicarse utilizando Bluetooth Low Energy (BLE).
   - *c*) El módulo debe utilizar un único chip que integre el microprocesador y la conectividad WiFi/Bluetooth.
   - *d*) El módulo debe contar como mínimo con interfaces de comunicación serie SPI (*Serial Peripheral Interface*), I2C (*Inter-Integrated Circuit*) y UART (*Universal Asynchronous Receiver-Transmitter*), a los fines de poder adaptarse a los distintos tipos de electrodomésticos.
3. Requerimientos de firmware.
   - *a*) El firmware del módulo debe ser programado en lenguaje C.
   - *b*) Se deben realizar pruebas manuales para cada una de las funcionalidades del firmware del módulo.
4. Requerimientos de gestión de proyectos.

a) Se debe utilizar YouTrack [21] como herramienta de *issue tracking* y gestión de proyectos.

b) Se debe usar Git como sistema de control de versiones.

Cabe mencionar en este punto que originalmente se había planteado la integración del módulo a un electrodoméstico real, lo que implicaba también el diseño y fabricación de un PCB que se adapte al mismo. Sin embargo, debido a las dificultades para acceder a un electrodoméstico sobre el cual probar el módulo, sumado a la necesidad de acelerar los tiempos de desarrollo, se decidió reemplazar dicho electrodoméstico por otro microcontrolador que emule su comportamiento.

2.5. Planificación

Para mostrar la planificación del trabajo, se recurre a un diagrama *Activity On Node* (figuras 2.3, 2.4 y 2.5), en el cual cada caja o nodo representa una actividad, y las conexiones entre ellas representan una dependencia temporal en la que una debe terminarse antes que la siguiente. Además se muestra el tiempo en horas que demoraría cada una de las tareas.

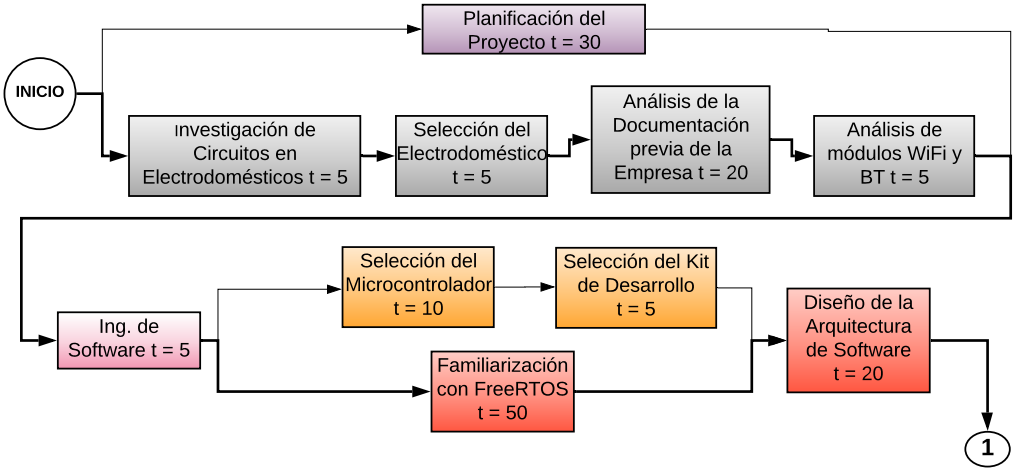

FIGURA 2.3: Diagrama Activity On Node Parte 1.

Se puede observar que la primera etapa consiste en análisis e investigación, además de la planificación del trabajo propiamente dicha. Luego sigue una etapa de diseño de firmware y familiarización con las herramientas a utilizar, sin empezar aún con la implementación.

Una vez definido el diseño, se procede con el desarrollo de las diferentes funcionalidades de firmware y sus respectivas pruebas. Si bien en el diagrama (figura 2.4) el desarrollo de estas tareas se muestra en paralelo, ya que son relativamente independientes y por lo tanto podrían ejecutarse en simultáneo, al ser desarrollado por una única persona, las tareas se debieron desarrollar en serie.

Luego se integran todas las funcionalidades implementadas y se realizan pruebas generales del sistema, para posteriormente configurar las plataformas utilizadas para enviar y recibir información por WiFi y Bluetooth.

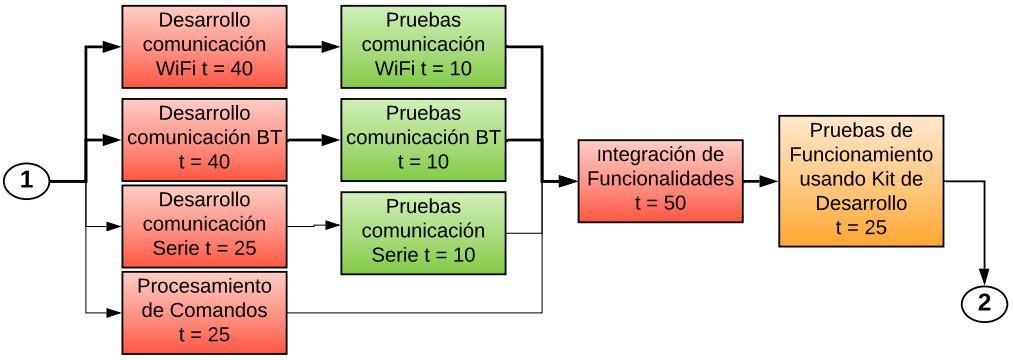

FIGURA 2.4: Diagrama Activity On Node Parte 2.

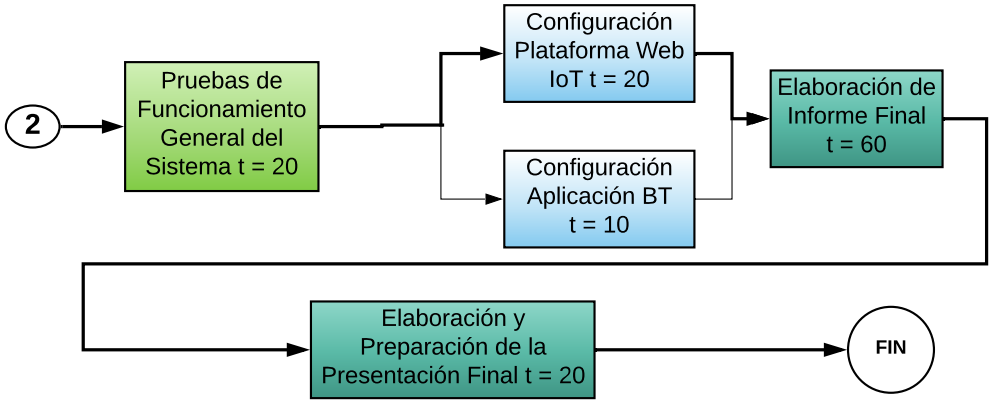

FIGURA 2.5: Diagrama Activity On Node Parte 3.

Finalmente se contempla también el tiempo necesario para las actividades asociadas a la presentación del trabajo final.

Capítulo 3

Diseño e Implementación

En este capítulo se describe el diseño e implementación de los diferentes módulos de firmware del sistema, como así también las diferentes herramientas utilizadas. También se presenta la interfaz para el usuario final y cómo el módulo se integra con los servicios de plataformas en la nube.

3.1. Herramientas utilizadas

En esta sección se detallan las diferentes herramientas y tecnologías utilizadas, tanto a nivel de hardware como de software embebido, justificando la elección en cada caso.

3.1.1. Hardware

La principal elección a nivel de hardware radica en el microcontrolador a utilizar en el módulo. Al momento de realizar la selección, se deben tener en cuenta numerosos factores tales como capacidad de procesamiento, memoria RAM, memoria flash, cantidad de pines GPIO (*General Purpose Input Output*, es decir entradas y salidas de propósito general), interfaces de comunicación, consumo de energía, costos y disponibilidad, entre otros. Lógicamente, algunos factores tendrán más importancia que otros dependiendo de la aplicación.

En el caso del módulo a desarrollar, los requerimientos planteados en la sección 2.4 ya imponen restricciones considerables en cuanto a las interfaces de comunicación. Por un lado, debido a la comunicación con la placa de control del electrodoméstico, el microcontrolador debe contar al menos con interfaces de comunicación serie UART, I2C y SPI. Además, para simplificar el desarrollo y lograr un diseño más compacto, se exige que el mismo chip cuente también con las interfaces para la comunicación WiFi y Bluetooth del módulo. Estos requerimientos en cuanto a interfaces reduce considerablemente el abanico de posibilidades.

Por otra parte, al tratarse de un módulo que potencialmente tendría acceso a la misma fuente de alimentación que el electrodoméstico, el consumo de energía no es un factor importante a tener en cuenta al momento de la elección.

Debido a que el trabajo consiste en el desarrollo de un prototipo, es sumamente importante que el microcontrolador cuente con un entorno de desarrollo robusto, tanto a nivel de placas o kits de desarrollo, como a nivel de herramientas de

programación. Tener esto cuenta al momento de la elección permite un ahorro sustancial de posterior tiempo de desarrollo.

Por todo lo expuesto anteriormente, es que se decide utilizar un ESP32 [22], el cual es un microcontrolador de 32 bits desarrollado por la compañía Espressif Systems y que cuenta con todas las interfaces de comunicación requeridas integradas en el mismo chip, tal como puede verse en la tabla 3.1.

TABLA 3.1: Interfaces de comunicación disponibles en un microcontrolador ESP32.

Interfaz de comunicación	Cantidad
WiFi	1
BLE	1
UART	3
SPI	4
I2C	2

Además el microcontrolador ESP32 cuenta con un excelente entorno de programación, numerosas placas de desarrollo, una documentación oficial de gran calidad y una comunidad muy activa.

En la figura 3.1 se puede observar la placa de desarrollo para ESP32 utilizada para el desarrollo de este trabajo, llamada NodeMCU [23]. Esta placa se eligió principalmente por su gran disponibilidad en el mercado local.

FIGURA 3.1: Placa de desarrollo para ESP32 NodeMCU.[1]

Cabe mencionar que la placa de desarrollo no utiliza directamente el microcontrolador ESP32, sino que usa el módulo ESP32-WROOM [24], el cual es un chip que posee en su interior un ESP32, pero contiene además una memoria flash de 4MB conectada a este y una antena de PCB integrada para la conectividad WiFi y Bluetooth, entre algunas otras funcionalidades.

[1]Imagen extraída de https://naylampmechatronics.com/espressif-esp/384-placa-de-desarrollo-para-esp32-nodemcu-32.html.

3.1.2. Software embebido

A nivel de software embebido, la principal decisión pasa por determinar si es necesario utilizar un sistema operativo de tiempo real (RTOS por sus siglas en inglés correspondientes a *Real Time Operating System*).

Si bien el módulo no requiere cumplir con restricciones de tiempo real, un RTOS ofrece otras atractivas características que justifican su uso. Entre estas características, la de mayor utilidad es la capacidad de gestionar la ejecución de múltiples tareas. Además ofrecen otras herramientas que resultan de gran utilidad como temporizadores o colas para comunicar tareas entre sí. También permiten integrar con mayor facilidad librerías que implementen funcionalidades complejas como los protocolos TCP/IP.

Por ello es que, dada la complejidad del sistema a implementar, en el que se requieren múltiples tareas ejecutándose y comunicándose entre sí, sumado a la necesidad de recurrir a una implementación del *stack* TCP/IP, se decide utilizar un sistema operativo de tiempo real.

A su vez existen numerosas alternativas al momento de determinar qué RTOS utilizar. Sin embargo, el microcontrolador ESP32 ya cuenta con todo un entorno de desarrollo denominado ESP-IDF (*Espressif IoT Development Framework*), el cual es una versión de FreeRTOS [25] modificada para trabajar de manera óptima con este microcontrolador. Por ello se decide utilizar este *framework* para el desarrollo del firmware y por lo tanto FreeRTOS como sistema operativo de tiempo real.

3.1.3. Plataforma en la nube

Para que el fabricante del electrodoméstico pueda almacenar, analizar y visualizar la información de sus diferentes electrodomésticos conectados, es sumamente conveniente recurrir a una plataforma de servicios en la nube. Estas plataformas se ocupan de gestionar toda la infraestructura necesaria asociada a la administración de dispositivos, autenticación, almacenamiento, análisis de datos, y mucho más.

Existen diferentes alternativas de plataformas que se pueden usar para lograr este objetivo, siendo las más conocidas las ofrecidos por Google (Google Cloud Platform [26]), Amazon (Amazon Web Services [27]) y Microsoft (Microsoft Azure [28]). En los tres casos tienen servicios similares orientados específicamente a la Internet de las Cosas: Google Cloud IoT Core, AWS IoT y Azure IoT, respectivamente. Un gran atractivo de las tres plataformas, es que ofrecen un saldo inicial considerable que permite utilizar sus servicios sin necesidad de incurrir en gastos. Además muchos servicios pueden ser utilizados sin costo indefinidamente, con ciertas restricciones en cuanto a recursos disponibles y con un consumo que debe mantenerse por debajo de ciertos valores. Esto permite probar las tres plataformas y atravesar toda la etapa de desarrollo y prototipado sin que ello sea un costo adicional.

Tras llevar a cabo un exhaustivo análisis para determinar cuál de las tres plataformas utilizar, y debido a que las tres plataformas cuentan con características muy similares, se decidió utilizar Google Cloud Platform principalmente por las siguientes causas:

- La autenticación de los dispositivos es más sencilla y utiliza mecanismos estándar.
- La curva de aprendizaje inicial es menos pronunciada, lo que permite agilizar el desarrollo.
- Los dispositivos se pueden comunicar tanto por HTTP/S como por MQTT.

Al utilizar Google Cloud Platform, se hace también un uso exhaustivo de Google Cloud IoT Core, el cual es un servicio completamente administrado que permite conectar, administrar y transferir datos con rapidez y seguridad desde millones de dispositivos (o desde tan sólo unos pocos) en todo el mundo [29]. Además, Google Cloud IoT Core puede combinarse con otros servicios de la plataforma, para así tener a disposición una solución completa para recopilar, procesar, analizar y visualizar datos de IoT en tiempo real.

3.2. Firmware

Para implementar las funcionalidades explicadas en la sección 2.1, fue necesario desarrollar a nivel de firmware diferentes módulos que interactúan entre sí, como puede verse en el diagrama de la figura 3.2. En la arquitectura planteada, cada uno de los módulos del diagrama se corresponde con una tarea que se ejecuta en el sistema operativo de tiempo real.

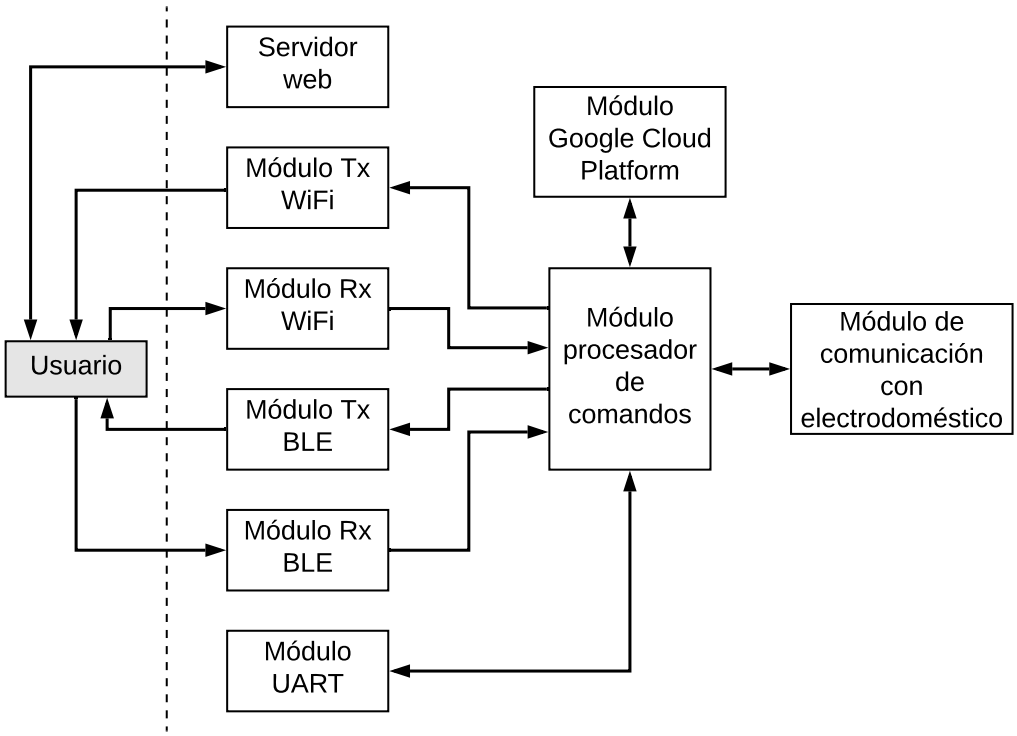

FIGURA 3.2: Diagrama de bloques de los módulos de firmware implementados.

De esta forma se tiene un módulo central (módulo procesador de comandos en el diagrama) que se encarga de recibir y procesar todos los comandos, y de generar todas las respuestas necesarias, abstrayéndose del origen o destino de los

mismos. Es decir que si el usuario del electrodoméstico manda un determinado comando por WiFi o Bluetooth, el módulo procesador de comandos es quien lo recibe en ambos casos, y luego se encarga de enviar la respuesta al módulo correspondiente (WiFi o Bluetooth según sea el caso). Además, este módulo es el único que interactúa con el módulo encargado de la comunicación con el electrodoméstico, por lo que toda comunicación con este debe pasar necesariamente a través del procesador de comandos. Esta centralización permite tener un gran control acerca de cómo ocurre la interacción entre los módulos y las prioridades al momento de atender más de una consulta. La sincronización y el pasaje de datos entre las diferentes tareas de cada módulo y el procesador de comandos se lleva a cabo mediante colas o *queues* [30].

Por otra parte, se tienen los módulos encargados tanto de recibir los comandos enviados por el usuario y enviarlos al módulo procesador de comandos, como así también de recibir las respuestas para enviarlas nuevamente al usuario. Estos son los módulos Tx (transmisor, es decir el que envía la respuesta al usuario) y Rx (receptor, es decir el que recibe el comando del usuario), tanto WiFi como Bluetooth. En secciones posteriores se profundiza más sobre la implementación específica de estos módulos, pero a grandes rasgos se ocupan de manejar toda la interacción necesaria con el hardware y los *drivers* asociados a la comunicación WiFi/Bluetooth. También se encargan de detectar el comando/respuesta recibido y enviarlo a donde corresponda.

Cabe mencionar que en el caso de los módulos WiFi, se cuenta con tres implementaciones diferentes, una para cada uno de los protocolos de aplicación soportados: HTTP, HTTPS y MQTT. Si bien en los tres casos se reutiliza en su totalidad todo lo asociado a la interacción con el hardware, la forma de enviar y recibir información difiere considerablemente. Además, solamente uno de los tres protocolos se puede soportar en simultáneo, debido principalmente a limitaciones de memoria RAM, que impide asignar el *stack* suficiente para todas las tareas a la vez. Por ello es que mediante banderas del compilador (*compiler flags*), se especifica qué protocolo usará la imagen de firmware generada.

En la figura 3.2 también se observa un módulo UART, que a diferencia de los otros módulos de transmisión y recepción, no interactúa con el usuario. Esto se debe a que es una tarea que se incluyó sólo con fines de *debug*, ya que permite enviar y recibir los mismos comandos que a través de las interfaces inalámbricas, pero de una forma mucho más simple utilizando una de las interfaces UART del microcontrolador.

Como se mencionó en la sección 3.1.3, para que el fabricante del electrodoméstico pueda analizar y visualizar la información de sus electrodomésticos conectados, se utiliza Google Cloud Platform. El módulo desarrollado envía periódicamente información acerca de su estado, para que luego esta información sea almacenada, analizada y visualizada a lo largo del tiempo. De esto precisamente se encarga el módulo Google Cloud Platform. Cada vez que la tarea requiere obtener el estado del electrodoméstico, lo hace a través del procesador de comandos, enviando un comando de manera muy similar a como lo haría el usuario.

Otro de los módulos involucrados en la comunicación WiFi es el del servidor web. Esta tarea se encuentra corriendo permanentemente de fondo, y permite que el usuario, conectándose a una red WiFi local generada por el propio microcontrolador (que actúa también como punto de acceso), ingrese a una página web que

permite configurar las credenciales de la red WiFi del hogar a la cual el módulo se debe conectar.

Finalmente, se tiene el módulo de comunicación con el electrodoméstico. Esta tarea se encuentra la mayor parte del tiempo bloqueada, esperando que el procesador de comandos se comunique con ella, con el objetivo de disparar alguna acción en el electrodoméstico. Una vez que lo hace, la tarea se comunica con el artefacto mediante la interfaz serie correspondiente. Dado que el electrodoméstico se emula mediante otro microcontrolador que cuenta con una interfaz I2C, ésta es la que se emplea para la comunicación serie.

3.2.1. Comunicación WiFi

Para lograr una comunicación con una página web externa en Internet desde el microcontrolador, es necesario contar con implementaciones de todas las capas del modelo TCP/IP. Para ello, se utilizaron en su mayor parte librerías ya existentes optimizadas para sistemas embebidos, tal como puede observarse en la tabla 3.2.

TABLA 3.2: Capas del modelo TCP/IP con sus correspondientes protocolos e implementaciones en el microcontrolador.

Capa del modelo TCP/IP	**Protocolo**	**Implementación**
Aplicación	HTTP/HTTPS/MQTT	ESP-IDF
Seguridad	TLS	mbed TLS
Transporte	TCP	lwIP
Internet	IP	lwIP
Acceso a la red	WiFi	ESP-IDF

Para manejar la comunicación a más bajo nivel mediante WiFi, se recurre al *driver* que forma parte del *framework* ESP-IDF desarrollado por el propio fabricante del microcontrolador. Este *driver* expone una API con ciertas funciones que el programador puede llamar para interactuar con la interfaz WiFi del chip. También se debe definir un *event handler* (manejador de eventos), es decir una función que el *driver* WiFi llama cada vez que debe notificar un nuevo evento que haya ocurrido. En la figura 3.3 se puede apreciar esta interacción entre el *driver* y el programa principal.

El *driver* WiFi permite utilizar la interfaz en tres modos diferentes:

- Modo estación (*station mode*) o modo cliente WiFi, en el que el microcontrolador se conecta a un punto de acceso.
- Modo punto de acceso (*AP mode*), en el que el microcontrolador actúa como un punto de acceso al que otros clientes se conectan.
- Modo combinado (*combined AP-STA mode*), en el que el microcontrolador se comporta como punto de acceso y a la vez como una estación que se conecta a otro punto de acceso.

En este trabajo se utiliza el modo combinado, ya que se requiere que el chip funcione como estación (para conectarse a la red WiFi del hogar que le da salida a

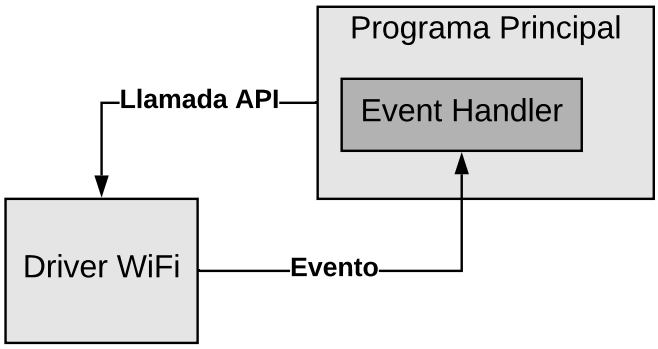

FIGURA 3.3: Interacción entre el driver WiFi y el programa principal.

Internet) y como punto de acceso (para que el usuario pueda acceder al servidor web que corre en el microcontrolador).

Con respecto al *event handler*, los eventos de interés que gestiona son los siguientes:

- STA_START: se dispara luego de que el driver se ha inicializado como estación. En este punto es posible conectarse a una red en particular.
- STA_GOT_IP: se dispara cuando se logra una conexión exitosa a una red y se obtiene una dirección IP.
- STA_DISCONNECTED: se genera cuando se produce una desconexión de la red.
- AP_START: se dispara luego de que el driver se ha inicializado como punto de acceso. En este punto se puede comenzar a ejecutar el servidor web.
- AP_STACONNECTED: se produce cuando una estación se conecta al punto de acceso.
- AP_STADISCONNECTED: se genera cuando una estación se desconecta del punto de acceso.

Muchas tareas necesitan tener conocimiento de los eventos que gestiona el *event handler*, principalmente requieren conocer cuándo el módulo ha logrado conectarse a la red deseada. Para lograr esta sincronización se utilizan *event groups* [31], cuyos bits se programan en el *event handler* del *driver* WiFi. Por ejemplo, cuando se establece una conexión exitosa a una red, el bit 0 del *event group* se pone en 1 y así se disparan de manera sincronizada aquellas tareas que estaban esperando que se establezca dicha conexión.

Continuando con las próximas capas del modelo, para las de Transporte/Internet, se hace uso de los protocolos TCP/IP. Para ello se utiliza la librería lwIP [32], que es una implementación de código abierto de los protocolos TCP/IP diseñada para sistemas embebidos, ya que busca minimizar al máximo la utilización de recursos.

El protocolo TCP/IP no proporciona ningún tipo de seguridad para la red en la que se los utiliza. Sin embargo, es posible agregar una capa adicional por encima

de la de transporte, que permita establecer una comunicación segura, encriptada y autenticada a lo largo de una red no segura. Esta seguridad adicional para la capa de transporte se denomina *Transport Layer Security* (TLS) [33] y para su implementación se recurre a la librería mbed TLS [34].

Finalmente, para la capa de aplicación se utilizan tres protocolos diferentes: HTTP, HTTPS y MQTT. En el caso de HTTPS y MQTT la comunicación es segura ya que se utiliza también TLS, mientrás que para el protocolo HTTP la información no se transmite de manera segura y podría ser interceptada en el camino.

Como ya se mencionó anteriormente, los tres protocolos no son soportados en forma simultánea, sino que en tiempo de compilación se decide cuál de ellos se va a usar en la imagen generada.

En el caso de los protocolos HTTP y HTTPS, si bien el *framework* ESP-IDF ya cuenta con implementaciones de clientes, se decide llevar a cabo una implementación propia a los fines de profundizar los conocimientos en la temática. Para ello, en el cliente HTTP se utiliza la librería lwIP para crear los *sockets* necesarios y realizar las escrituras y lecturas necesarias, creando métodos para enviar una HTTP *request* y recibir una HTTP *response*. El caso del cliente HTTPS es más complejo, y se utiliza la libreria mbed TLS para crear todas las estructuras necesarias para la transacción segura, y luego también se definen métodos para enviar *requests* y recibir *responses*, incluyendo el proceso del *handshake* TLS [35].

Una vez implementados los clientes HTTP y HTTPS, se los utiliza en los respectivos módulos de transmisión y recepción de comandos por WiFi. Las tareas implementadas son relativamente sencillas y muy similares para ambos protocolos, diferenciándose principalmente en las funciones que llaman para enviar y recibir información. En la figura 3.4 se puede apreciar un diagrama de flujo de la tarea de transmisión por WiFi usando HTTP/HTTPS. Cabe mencionar que el que envía datos nuevos a la cola de la tarea es el procesador de comandos, cuando desea devolver una respuesta al usuario.

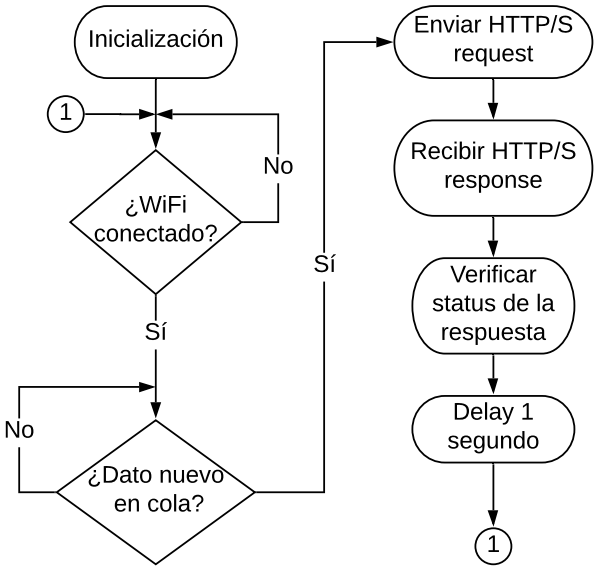

FIGURA 3.4: Diagrama de flujo para las tareas de transmisión por HTTP/HTTPS.

Por otra parte, en la figura 3.5 se observa un diagrama de flujo de las tareas de recepción de comandos empleando HTTP/HTTPS. El funcionamiento básico de esta tarea consiste en consultar periódicamente si el usuario ha enviado un nuevo comando, y en caso afirmativo reenviarlo al procesador de comandos.

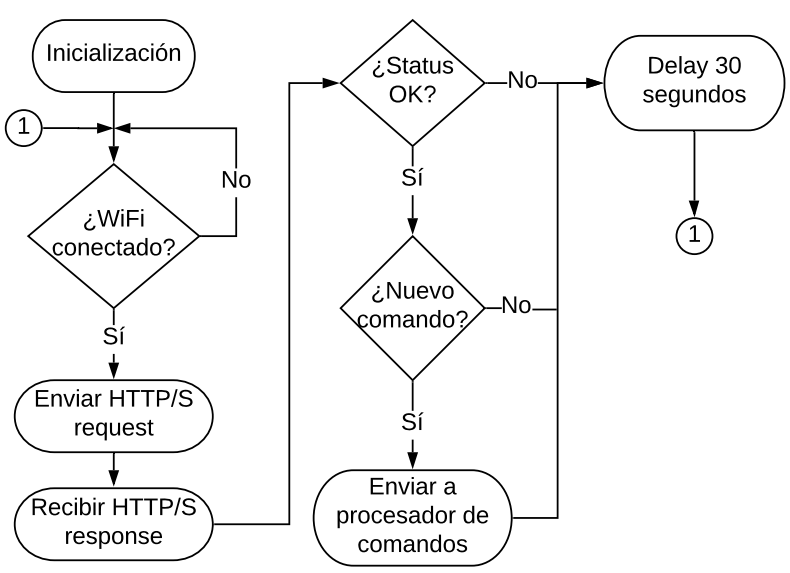

FIGURA 3.5: Diagrama de flujo para las tareas de recepción por HTTP/HTTPS.

Finalmente, para el caso de los módulos WiFi con protocolo MQTT, se decide utilizar directamente las implementaciones del protocolo que ya forman parte del *framework* ESP-IDF, debido a que una implementación propia resultaría demasiado compleja y escapa al alcance de este trabajo. El funcionamiento general de las tareas es análogo al de las versiones con HTTP/HTTPS, con la diferencia de que ahora se utiliza MQTT para publicar las respuestas hacia el usuario en un *topic* determinado, y recibir comandos desde otro *topic* al cual el microcontrolador se encuentra subscripto. El protocolo MQTT se utiliza sobre TLS, por lo tanto todos los intercambios de información ocurren de manera segura.

De manera similar al *driver* WiFi, se implementa un *event handler* que gestiona los siguientes eventos asociados al protocolo MQTT:

- MQTT_EVENT_CONNECTED: se dispara cuando se logra una conexión exitosa con el *broker* MQTT.
- MQTT_EVENT_DISCONNECTED: se genera ante una desconexión del *broker*.
- MQTT_EVENT_SUBSCRIBED/UNSUBSCRIBED/PUBLISHED: se produce cada vez que un cliente MQTT se suscribe, elimina la suscripción o publica datos en un *topic* determinado.
- MQTT_EVENT_DATA: se genera cada vez que un *topic*, al que algún cliente se encuentra suscripto, recibe información nueva y la envía al cliente MQTT.

3.2.2. Comunicación BLE

Un dispositivo BLE puede actuar como *peripheral* (periférico o servidor) o como *central* (principal o cliente), y en el caso de este trabajo el microcontrolador actúa como un *peripheral*. El servidor anuncia continuamente su presencia, enviando paquetes para que otros dispositivos detecten su presencia. Por su parte, el dispositivo *central*, que en este caso sería la aplicación en el celular del usuario del electrodoméstico, realiza un escaneo en busca de dispositivos cercanos. Una vez que encuentra el *peripheral* deseado, establece una conexión y le realiza diferentes peticiones.

De manera similar al caso del WiFi, se cuenta con un *driver* que gestiona la interfaz Bluetooth y se comunica con el programa principal mediante eventos. En este caso se deben definir varios *event handlers* para gestionar diferentes facetas de la comunicación. Para entender el funcionamiento de la comunicación BLE implementada es necesario comprender también algunos conceptos asociados al propio protocolo.

Por un lado se tiene el concepto de GAP (*Generic Access Profile*), que controla las conexiones y el *advertising*, es decir cómo el servidor anuncia su presencia transmitiendo paquetes periódicamente. Mediante las estructuras de datos y funciones que el *framework* expone, se especifican diferentes parámetros como el *advertising interval* (cada cuánto el dispositivo anuncia su presencia) o el nombre del dispositivo, entre muchos otros. Además se tiene un *event handler* para los eventos asociados al GAP, entre los que se destacan dos en particular:

- GAP_BLE_ADV_DATA_SET_COMPLETE_EVT: se dispara cuando los parámetros de *advertising* se encuentran configurados, y por lo tanto se lo utiliza para iniciar el proceso de *advertising*. Es decir que cuando este evento se detecta, el dispositivo comienza a anunciar su presencia.
- GAP_BLE_ADV_START_COMPLETE_EVT: este evento indica que el proceso de *advertising* terminó su inicialización, y se lo puede utilizar para determinar si dicha inicialización tuvo éxito u ocurrió alguna falla.

En cuanto a la forma de transmitir datos, el intercambio de información entre dos dispositivos BLE se realiza mediante los denominados atributos genéricos o GATT (*Generic Attributes*), los cuales son estructuras de datos jerárquicas que constituyen la base del protocolo. Esta jerarquía puede observarse en la figura

En cuanto a la forma de transmitir datos, el intercambio de información entre dos dispositivos BLE se realiza mediante los denominados atributos genéricos o GATT (*Generic Attributes*), los cuales son estructuras de datos jerárquicas que constituyen la base del protocolo. Esta jerarquía puede observarse en la figura 3.6 y está constituida por varias partes:

- Perfil (*profile*): es la jerarquía de mayor nivel y está formada por uno o más servicios.
- Servicio (*service*): es un conjunto de diferentes informaciones (como lecturas de un sensor), y contiene por lo menos una característica. Existen numerosos servicios predefinidos por el Bluetooth Special Interest Group (SIG), como presión sanguínea o ritmo cardíaco, y además se pueden crear servicios personalizados en caso de que el uso no esté contemplado en esa lista predefinida, como es el caso de este trabajo.

- Característica (*characteristic*): es donde se encuentran los datos propiamente dichos. Posee varios campos, entre los que se destacan el de *value*, con el valor en sí, y el de *properties*, que describe cómo se puede interactuar con el valor.

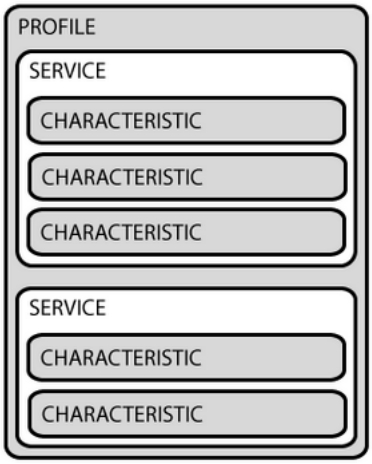

FIGURA 3.6: Jerarquía de la estructura GATT.[2]

Un cliente puede llevar a cabo diferentes operaciones sobre una característica de un *peripheral*, incluyendo operaciones de lectura y escritura. Esto justamente es lo que se utiliza para enviar comandos por BLE (se escribe una característica en particular) y para recibir respuestas (se lee una característica).

Se implementa también un *event handler* para los eventos asociados a GATT, entre los cuales se destacan los siguientes:

- GATTS_REG_EVT: es el primer evento que se dispara al iniciar el servidor BLE. Se lo utiliza para configurar los parámetros de *advertising* (lo cual dispara luego el correspondiente evento en el *event handler* de GAP) y para crear el servicio que usa la aplicación.
- GATTS_CREATE_EVT: es el próximo evento en dispararse luego de que el servicio se crea exitosamente. Se lo usa para iniciar el servicio y para agregarle las características que luego se usan para enviar comandos y recibir respuestas.
- GATTS_CONNECT_EVT/GATTS_DISCONNECT_EVT: se dispara cada vez que un cliente se conecta/desconecta del *peripheral*.
- GATTS_WRITE_EVT: se produce cuando el dispositivo cliente desea realizar una operación de escritura sobre una característica, es decir cuando el usuario desea mandar un comando al electrodoméstico. En este punto se lee lo que el usuario escribió en la característica y se lo envía al procesador de comandos.
- GATTS_READ_EVT: se produce cuando el cliente desea realizar una operación de lectura sobre una característica, es decir cuando el usuario desea recibir una respuesta del electrodoméstico. Para ello se escribe en la característica correspondiente el valor que se recibe desde el procesador de comandos.

[2]Imagen extraída de https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gatt.

3.2.3. Procesamiento de comandos

La tarea que se encarga de procesamiento de comandos se encuentra en todo momento que algún módulo escriba en la cola correspondiente. Se utiliza una única cola a la que todos los módulos envían datos, a través de una estructura que incluye no solamente el comando propiamente dicho, sino también un identificador del módulo que escribió en la cola, tal como puede verse en el algoritmo 3.1.

```
/*-------------------------------------------------------------------
|  Struct: rx_command_t
| -------------------------------------------------------------------
|  Description: represents a received command.
|
|  Members:
|       rx_id   - module that sent the command
|       command - command received
*-------------------------------------------------------------------*/
typedef struct {
    rx_module_t     rx_id;
    command_type_t  command;
}   rx_command_t;
```

ALGORITMO 3.1: Pseudocódigo del lazo principal de control.

Cuando se necesita enviar una respuesta, se utiliza ese *rx_id* para determinar el módulo adecuado y por lo tanto en qué cola se debe escribir la respuesta.

El tipo de dato *command_type_t* define los diferentes comandos disponibles, y es fácilmente extensible con nuevos valores. Existen dos grupos de comandos:

- Comandos dirigidos al módulo: no se comunican con el electrodoméstico, sino que actúan solamente sobre el módulo de conectividad.
  - CMD_WIFI: se utiliza para cambiar el estado de la conexión WiFi (si está apagada la enciende, si está encendida la apaga). Debido a que el WiFi y el BLE no pueden estar funcionando en simultáneo, en caso de que este último se encuentre encendido, se lo desactiva antes de iniciar la conexión WiFi.
  - CMD_BLE: análogo a CMD_WIFI, pero aplicado a Bluetooth Low Energy.
  - CMD_ECHO: comando utilizado para *debug*, simplemente le devuelve a la misma interfaz los mismos datos que envió.
- Comandos dirigidos al electrodoméstico: son una serie de comandos genéricos a modo de ejemplo, los cuales se envían por I2C al microcontrolador que emula al electrodoméstico.
  - CMD_SLAVE_START_A/CMD_SLAVE_START_B: inicia en el electrodoméstico un determinado proceso.
  - CMD_SLAVE_PAUSE: pausa el proceso actual.
  - CMD_SLAVE_CONTINUE: reanuda un proceso pausado.
  - CMD_SLAVE_RESET: reinicia el electrodoméstico.
  - CMD_SLAVE_STATUS: se lo emplea para preguntar por el estado actual del electrodoméstico.

Para el microcontrolador que emula el comportamiento del electrodoméstico, el cual también es un ESP32, se desarrolló un firmware simplificado con una tarea principal que consiste en una máquina de estados, la cual representa los diferentes estados del electrodoméstico. Los comandos que recibe por su interfaz I2C pueden modificar esta máquina de estados, reflejando así que un determinado proceso inicia o termina. Además, cada vez que recibe un comando desde el módulo principal, le devuelve al mismo una señal de *acknowledge*, la cual es verificada por la tarea de procesamiento de comandos cada vez que se produce una comunicación con el electrodoméstico.

3.3. Integración con Google Cloud Platform

Como se mencionó en la sección 3.1.3, para proporcionarle información al fabricante acerca del estado del electrodoméstico se utiliza Google Cloud Platform. Esta implementación tiene dos facetas: por un lado la tarea a nivel de firmware que permite que el microcontrolador se comunique con Google Cloud, y por el otro toda la infraestructura y los servicios utilizados en Google Cloud.

Se utilizan diferentes servicios de Google Cloud Platform, y el principal de ellos es Cloud IoT Core. Este servicio cuenta con dos componentes principales:

- *Device manager* (administrador de dispositivos): permite registrar y administrar dispositivos, y ofrece también un mecanismo para autenticarlos cuando se conectan. El módulo desarrollado se registra aquí como dispositivo.
- *Protocol bridge* (puente de protocolos): permite acceder a Google Cloud de manera segura mediante protocolos MQTT y HTTP.

El servicio de Cloud IoT Core interactúa con varios otros servicios de Google Cloud para armar un flujo de análisis completo, como puede observarse en la figura 3.7.

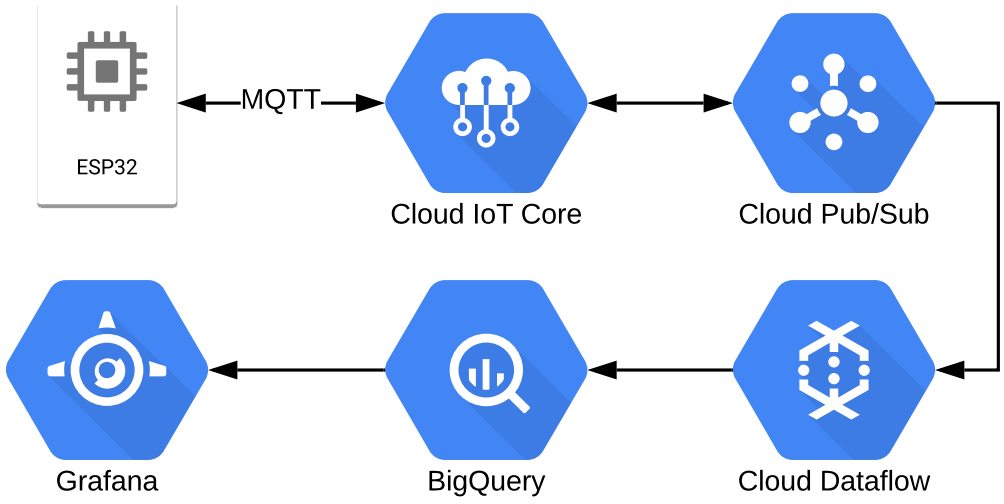

FIGURA 3.7: Arquitectura utilizada en Google Cloud Platform.

El servicio más importante con el que interactúa es Cloud Pub/Sub, ya que es el servicio en el cual se publican todos los datos recibidos por el *protocol bridge*.

De hecho cada dispositivo en Cloud IoT Core tiene asociado al menos un *topic* en Cloud Pub/Sub, y es en ese *topic* donde el microcontrolador realiza la publicación de los datos que desee.

En este punto ya se tiene almacenada toda la información cruda enviada por el electrodoméstico, y los bloques restantes se encargan de mostrar gráficamente esa información utilizando Grafana, que es una herramienta que permite la visualización de datos provenientes de distintas fuentes. En este caso se utiliza como fuente Big Query, una base de datos altamente eficiente y escalable ofrecida por Google Cloud. Para que los datos de los *topics* se transfieran y almacenen automáticamente a la base de datos, se utiliza Cloud Dataflow. Finalmente se utiliza la propia infraestructura de Google Cloud para levantar la aplicación de Grafana, pudiendo así finalmente visualizar los datos enviados por el dispositivo.

Por otro lado, a nivel de firmware se cuenta con una tarea dedicada exclusivamente a enviar periódicamente a Google Cloud información acerca del estado actual del electrodoméstico. Esta transmisión se lleva a cabo solamente utilizando el protocolo MQTT, es decir que no hay soporte para HTTP/HTTPS.

El principal desafío para enviar la información está en las autenticaciones necesarias para que esto sea posible.

Por un lado, debido a que la transmisión es segura (utiliza TLS por debajo) es necesario utilizar los certificados de Google Cloud Platform al momento de configurar el cliente MQTT. Esto no difiere del procedimiento realizado para las tareas de MQTT que interactúan con el usuario.

También es necesario autenticar el dispositivo en particular, es decir el microcontrolador debe demostrar que cuando se comunica con Google Cloud, es el dispositivo que dice ser y no otro haciéndose pasar por él [36]. Para ello es necesario generar claves, asociar dichas claves a cada dispositivo en Cloud IoT Core, y luego almacenar la clave también en el firmware. La figura 3.8 ilustra este proceso.

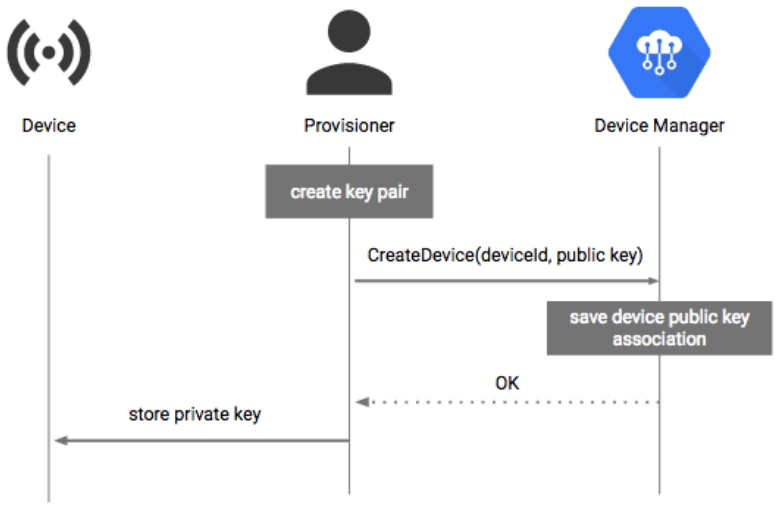

FIGURA 3.8: Proceso de generación de claves para el servicio de Cloud IoT Core.[3]

[3]Imagen extraída de https://cloud.google.com/iot/docs/concepts/device-securityprovisioning_credentials.

Luego el firmware debe utilizar la clave que tiene almacenada para generar un JSON Web Token (JWT) [37] y enviarlo al momento de conectarse por MQTT, como se observa en la figura 3.8.

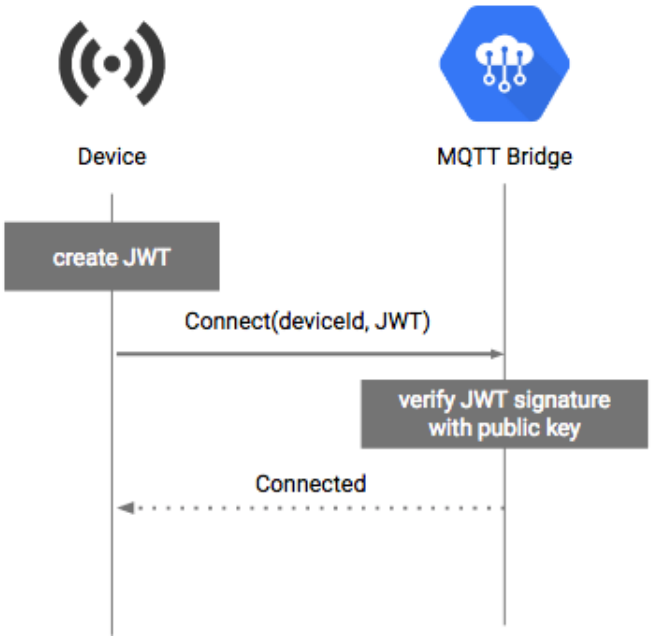

FIGURA 3.9: Autenticación del dispositivo utilizando un JWT.[4]

[4]Imagen extraída de https://cloud.google.com/iot/docs/concepts/device-securityprovisioning_credentials.

Capítulo 4

Ensayos y Resultados

Párrafo introductorio.

4.1. Pruebas funcionales

4.1.1. Comunicación WiFi

Servidor web

4.1.2. Comunicación BLE

4.1.3. Comunicación serie con electrodoméstico

4.2. Integración del sistema

4.2.1. Visualización de datos en Google Cloud Platform

Capítulo 5

Conclusiones

5.1. Conclusiones generales

5.2. Próximos pasos

Bibliografía

[1] IHS Markit. *The Internet of Things: a movement, not a market*. 2017.

[2] Statista. *Forecast end-user spending on IoT solutions worldwide from 2017 to 2025*. https://www.statista.com/statistics/976313/global-iot-market-size/. 2017. (Visitado 14-03-2020).

[3] Cloudflare. *What is the Mirai Botnet?* https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/. (Visitado 15-03-2020).

[4] Zack Whittaker. *CIA, MI5 hacked smart TVs to eavesdrop on private conversations*. https://www.zdnet.com/article/how-cia-mi5-hacked-your-smart-tv-to-spy-on-you/. 2017. (Visitado 15-03-2020).

[5] Danny Palmer. *Ransomware, snooping and attempted shutdowns: see what hackers did to these systems left unprotected online*. https://www.zdnet.com/article/ransomware-snooping-and-attempted-shutdowns-the-state-of-this-honeypot-shows-what-hackers-do-to-systems-left-unprotected-online/. 2020. (Visitado 15-03-2020).

[6] https://thingsboard.io/. (Visitado 18-03-2020).

[7] https://thinger.io/. (Visitado 18-03-2020).

[8] https://ubidots.com/. (Visitado 18-03-2020).

[9] *ThingWorx*. https://www.ptc.com/-/media/Files/PDFs/IoT/ThingWorx-Connect-Product-Brief.pdf. (Visitado 18-03-2020).

[10] https://www.particle.io/. (Visitado 18-03-2020).

[11] Asociación Española de Domótica e Inmótica. *Qué es Domótica*. http://www.cedom.es/sobre-domotica/que-es-domotica. (Visitado 17-03-2020).

[12] *NB-IoT, la nueva revolución del mundo conectado*. https://accent-systems.com/es/nb-iot. (Visitado 24-03-2020).

[13] Semtech. *What is Lora?* https://www.semtech.com/lora/what-is-lora. (Visitado 24-03-2020).

[14] Sigfox. *Sigfox technology*. https://www.sigfox.com/en/what-sigfox/technology. (Visitado 24-03-2020).

[15] *Wifi*. https://es.wikipedia.org/wiki/Wifi. (Visitado 24-03-2020).

[16] *Learn about Bluetooth Technology*. https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/. (Visitado 24-03-2020).

[17] *TCP/IP*. https://es.ccm.net/contents/282-tcp-ip-que-significa-tcp-ip. (Visitado 25-03-2020).

[18] *Generalidades del protocolo HTTP*. https://developer.mozilla.org/es/docs/Web/HTTP/Overview. (Visitado 25-03-2020).

[19] *HTTPS*. https://es.ryte.com/wiki/HTTPS. (Visitado 25-03-2020).

[20] *¿Qué es MQTT? Su importancia como protocolo IoT*. https://www.luisllamas.es/que-es-mqtt-su-importancia-como-protocolo-iot/. (Visitado 25-03-2020).
[21] *YouTrack*. https://www.jetbrains.com/es-es/youtrack/. (Visitado 22-03-2020).
[22] *ESP32, a different IoT power and performance*. https://www.espressif.com/en/products/hardware/esp32/overview. (Visitado 26-03-2020).
[23] *NodeMCU ESP32*. https://www.infootec.net/nodemcu-esp32/. (Visitado 28-03-2020).
[24] *ESP32 WROOM Series*. https://www.espressif.com/en/products/hardware/esp-wroom-32/overview. (Visitado 28-03-2020).
[25] *FreeRTOS, Real-time operating system for microcontrollers*. https://www.freertos.org/. (Visitado 28-03-2020).
[26] https://cloud.google.com.
[27] https://aws.amazon.com/.
[28] https://azure.microsoft.com/es-es/.
[29] *Cloud IoT Core*. https://cloud.google.com/iot-core. (Visitado 29-03-2020).
[30] *FreeRTOS Queues*. https://www.freertos.org/Embedded-RTOS-Queues.html. (Visitado 29-03-2020).
[31] *Event Bits (or flags) and Event Groups*. https://www.freertos.org/FreeRTOS-Event-Groups.html. (Visitado 29-03-2020).
[32] *lwIP - A Lightweight TCP/IP stack*. http://savannah.nongnu.org/projects/lwip/. (Visitado 29-03-2020).
[33] *Seguridad de la capa de transporte*. https://es.wikipedia.org/wiki/Seguridad_de_la_capa_de_transporte. (Visitado 29-03-2020).
[34] https://tls.mbed.org/. (Visitado 29-03-2020).
[35] *What happens in a TLS handshake?* https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/. (Visitado 30-03-2020).
[36] *Device security*. https://cloud.google.com/iot/docs/concepts/device-securityprovisioning_credentials. (Visitado 31-03-2020).
[37] *Introduction to JSON Web Tokens*. https://jwt.io/introduction/. (Visitado 31-03-2020).